September 20, 2021

Marlene Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: Notice of Proposed Rulemaking, *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232

Dear Ms. Dortch:

The undersigned organizations address proposals by the Federal Communications Commission ("FCC") in the *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program* Notice of Proposed Rulemaking.[1] Each association supports the objective behind the NPRM—preserving the integrity of U.S. communications networks against foreign adversaries and nation states.

Our organizations represent the breadth of the American and trusted allies' communications and technology sectors. Our member companies are engines of innovation, which has made the United States a global tech leader. We understand the importance of security and appreciate the need to safeguard American communications networks from foreign threats, as Congress and the FCC have been doing.[2] However narrow the proposed rules may seem, the NPRM raises a number of implementation and legal questions that the Commission should carefully consider before moving forward. Regulatory caution is particularly warranted because Congress is actively legislating on the specific question of access to the FCC's equipment authorization process by the companies identified by the FCC.[3]

As described in the NPRM, the new rules may be difficult to implement and may have serious unintended consequences. At least two of the proposals merit particular caution.

---

[1] ET Docket No. 21-232, FCC 21-73 (rel. June 17, 2021) ("NPRM"). The parties write separately to address the issues raised in the Notice of Inquiry, which is not focused on known threats from specific entities but instead proposes a much broader set of initiatives aimed at less well-defined concerns involving cybersecurity generally.

[2] *See* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609); *Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019).

[3] *See* Secure Equipment Act of 2021, S.1790, 117th Cong. (2021) (as introduced in Senate May 24, 2021).

First, revocation of existing authorizations raises serious implementation challenges for varied devices and components in use today—including by users, including consumers and enterprises. For example, devices and components potentially subject to revocation may be in homes or offices, or may be incorporated into other equipment used throughout the economy. How would users be made aware of the revocation? What impact would revocation have on existing devices in the field? How will users identify, source, and replace devices subject to revocation, and would assistance be provided in doing so? Devices sold at retail may be difficult or impossible to locate, and if a device has been incorporated into other equipment, a replacement may require new engineering, testing, validation, and manufacture.

Second, the NPRM's proposed criteria for evaluating a device relates to the origin and pedigree of the device rather than its technical characteristics. Enacting these criteria would require gatekeeping a far larger scope of equipment for far different considerations than the FCC has traditionally examined. For example, subjecting previously exempt low-emission devices to new regulation would bring millions more devices into the equipment authorization regime, creating administrative burdens for the FCC, manufacturers, and operators. The volume of devices that could now be subject to equipment authorization is vast. These low-emission devices have not previously been a source of significant concern for the agency, because when judged under the Commission's traditional purview of the technical impacts of radiofrequency emissions, they pose very little risk of disruption.

The proposed changes to the equipment authorization rules will strain vital resources in the FCC's Office of Engineering and Technology ("OET"). Indeed, the sheer number of devices that could be subject to review under the NPRM could require additional staffing and the development of new areas of expertise. The changes may also have unpredictable impacts on global trade and mutual recognition agreements that expedite global trade in telecommunications equipment.

Finally, the FCC's legal authority to take the actions contemplated in the NPRM is unclear. The NPRM proposes a type of review that the agency has not in the past conducted, breaking new legal ground. As the NPRM itself observes, the Commission's equipment authorization regime has historically been confined to technical characteristics of devices and certain matters specifically enumerated by Congress. But Congress has not directed the FCC to take the steps set out in the NPRM. And while the NPRM identifies the Secure Networks Act[4] as a potential source of authority, the fact that Congress is considering legislation to exclude certain organizations from equipment authorization[5] calls into question the claim that the FCC has existing authority under the Secure Networks Act or otherwise.

As representatives of America's broadband and technology future, we are eager to ensure that Americans continue to have access to safe and secure communications networks. We urge the Commission to be cautious as it considers how to address complex nation security and cybersecurity questions and best focus the FCC's expertise and resources to preserve the integrity of U.S communications networks.

---

4 *See* 47 U.S.C. § 1601 *et seq*.

5 *See* Secure Equipment Act of 2021, S.1790, 117th Cong. (2021) (as introduced in Senate May 24, 2021).

We look forward to continuing to work with the FCC on important policy matters affecting the communications and emerging technology sectors.

Respectfully submitted,

ACT – The App Association
Consumer Technology Association
Council to Secure the Digital Economy
CTIA
Internet Association
Information Technology Industry Council
U.S. Chamber of Commerce
USTelecom